****

**Universiti Teknologi MARA**

**Faculty of Computer & Mathematical Sciences**

**COMPUTER SECURITY (CSC662)  
RAIL FENCE CIPHER  
  
GROUP MEMBERS**

|  |  |  |
| --- | --- | --- |
| **Name** | **Student Id** | **Group** |
| **Wan Putera Nur Syafiq bin Wan Jeferi** | **2020836988** | **CS2306C** |
| **Azri Mustaqim bin Mohd Roslan** | **2020957741** | **CS2306C** |
| **Muhamad Arif Fikri bin Mustapa** | **2020461922** | **CS2306C** |
| **Nur Alia binti Mat Zani** | **2020455644** | **CS2306C** |
| **Nur Syafiqah Dayana binti Mohd Ridhuan** | **2020455788** | **CS2306C** |
| **Airani Natasha binti Mohd Anis** | **2020608242** | **CS2306C** |

**Prepared for**

**Sir Wan Ya Wan Hussin**

**Submission Date**

**24 July 2022**

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| **[Introduction](https://docs.google.com/document/d/1XPU4Sgre7X8gmKiNE2Bv93eWlMXnotQU43aCVGXHszE/edit" \l "heading=h.mijfu7nbq9cx)** | **3** |
| **Output** | **4** |
| **Advantages and Disadvantages** | **5** |
| **Improvement** | **6** |
| **Conclusion** | **6** |

1. **INTRODUCTION**

The rail fence cipher is an easy to apply transposition cipher that jumbles up the order of the letters of a message in a quick convenient way. It also has the security of a key to make it a little bit harder to break. The rail fence cipher also called a zigzag cipher is a form of transposition cipher. It derives its name from the way in which it is encoded.  In the rail fence cipher, the plaintext is written downwards diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached, down again when the top rail is reached, and so on until the whole plaintext is written out. The ciphertext is then read off in rows.

As for encryption using rail fence cipher, to encrypt a message, the message must be written in zigzag lines across the page, and then read off each row. Firstly, it needs to have a key, which for this cipher is the number of rows it is going to have. Start with writing the letters of the plaintext diagonally down to the right until it reaches the number of rows specified by the key and then bounces back up diagonally until it hit the first row again. This continues until the end of the plaintext.

1. **Findings**

First the user needs to enter the plaintext and key. The key will determine the rows that will be used. Based on the table 1.1 below, there is two examples that be used.

**Table 1.1** Output

|  |  |
| --- | --- |
| **Input** | **Output** |
| PT = COMPUTERSECURITY  Key = 5 | **Text  Description automatically generated** |
| PT = ILOVECRYPTOGRAPHY  Key = 4 | **Chart, scatter chart  Description automatically generated** |

1. **Advantages and Disadvantages**

Advantages:

* The advantage of the Rail Fence cipher over other transposition ciphers like the sawtooth cipher is that there is a variable distance between consecutive letters. What it means by variable distance is that the letters need not be arranged in fixed vertical columns that descends, but it can also be arranged in a zig zag manner. Therefore, this increases the difficulty of cracking the code. The rail fence cipher is being decrypted by reading it in arranging it in columns or rows before reading it. Therefore, it is quite an easy and fast process, and it is less prone to mistakes.

Disadvantages:

* Rail Fence Cipher security is very weak. The weakness can be seen from the lack of key. The number of practical keys is small enough that a cryptanalyst can break. It allows mixing up of characters in plaintext to produce the ciphertext, it offers essentially no communication security and will be shown that it can be easily broken. It cannot be used to encrypt images containing large areas of single colour. Another problem with the rail fence cipher is that is not very strong. This means that the number of possible solutions is so small that a cryptanalyst can try them all by hand. Therefore, the rail fence cipher is very easy to break as we only must test all the possible divisors up to half the length of the text.

1. **Improvement on Rail Fence Cipher**

By eliminating spaces, numbers, and symbols, the current rail fence encrypts plain text. No part of this encryption is represented by a space, number, or symbol. For brief messages, it performs pitiably. Inadequate keys are the cause of this. The suggested algorithm overcomes the restriction by engaging in three separate phases:

**Phase 1:** Substitution by using a unique symbol to represent plain text.

**Phase 2:** Transposition by doing circular shift.

**Phase 3:** Transposition by using rail fence.

**Procedure for Encryption**

**Step 1**: Read the plain text (PT)

**Step 2**: As a key, choose a random integer (K).

**Step 3**: Each character is represented by a unique symbol as seen in the Figure 1.1.

A screenshot of a computer

Description automatically generated with medium confidence

**Figure 1.1** Substitution Chart

**Step 4**: If the key value is even, a circular left shift operation is performed by K positions, and a circular right shift operation is performed by K positions if the key value is odd. K is used to donates the key-value.

**Step 5**: A series of diagonals or zigzags is used to write the message that results from the previous steps.

**Step 6**: Reading it row by row in the final stage will yield the output cypher text (C).

**Procedure for Decryption**

**Step 1:** Input Key (K) and the Cipher(C).

**Step 2:** Create a decryption matrix. The matrix's dimensions will be key-value (total rows) and cypher text size (total columns). The leading letter will be inserted in the top left corner of the matrix and run from corner to corner downward by placing a dash (-). Later, the other cypher letters will replace these dashes (-). The following character of the cypher will then be added, returning to the top row. Continue doing this within the row and then skip to the next row until we reach the finish. Afterward, we read it diagonally.

**Step 3:** Based on the key-value (even/odd), performs the circular shift operation (circular right shift/circular left shift) by K places.

**Step 4:** Using the letter shown in Figure 1.1, each symbol in the text obtained in Step 3 will be changed to a letter.

**Step 5:** After changing each character, the desired plain text (PT) is restored.

**Example of encryption**

Plaintext (PT): Rail Fence

Key: 3 (Odd)

|  |  |  |
| --- | --- | --- |
| Step 1 | Plain text (PT) | Rail Fence |
| Step 2 | Key (K) | 3 |
| Step 3 | Use a unique symbol to indicate the Plain Text (PT) | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | R | a | i | l |  | F | e | n | c | e | | % | ÷ | α | Δ | π | ; | φ | μ | ∞ | φ | |
| Step 4 | Because of the key is odd, perform a circular right shift by 3 positions | Before   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | % | ÷ | α | Δ | π | ; | φ | μ | ∞ | φ |   After   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | μ | ∞ | φ | % | ÷ | α | Δ | π | ; | φ | |
| Step 5 | Create zigzag sequence | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | μ |  |  |  | ÷ |  |  |  | ; |  | |  | ∞ |  | % |  | α |  | π |  | φ | |  |  | φ |  |  |  | Δ |  |  |  | |
| Step 6 | Read it row by row | Row 1: μ÷;  Row 2: ∞% α π φ  Row 3: φ Δ |
| Step 7 | Cipher text (C) | μ÷;∞% α π φ φ Δ |

**Example of decryption**

|  |  |  |
| --- | --- | --- |
| Step 1 | Cipher text | μ÷;∞% α π φ φ Δ |
| Step 2 | Key(K) | 3 |
| Step 3 | Read the cipher character diagonally after creating a diagonal matrix. | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | μ |  |  |  | - |  |  |  | - |  | |  | - |  | - |  | - |  | - |  | - | |  |  | - |  |  |  | - |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | μ |  |  |  | ÷ |  |  |  | ; |  | |  | ∞ |  | % |  | α |  | π |  | φ | |  |  | φ |  |  |  | Δ |  |  |  | |
| Step 4 | Perform a circular left shift by 3 positions. Because the key is odd. | Before   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | μ | ∞ | φ | % | ÷ | α | Δ | π | ; | φ |   After   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | % | ÷ | α | Δ | π | ; | φ | μ | ∞ | φ | |
| Step 5 | Replace the symbol by character | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | % | ÷ | α | Δ | π | ; | φ | μ | ∞ | φ | | R | a | i | l |  | F | e | n | c | e | |
| Step 6 | Plain Text (PT) | Rail Fence |

1. **Conclusion**

The Rail Fence Cipher is a very easy to apply transposition cipher. However, it is not particularly secure, since there are a limited number of usable keys, especially for short messages for there to be enough movement of letters, the length of the message needs to be at least twice the key, but preferably 3 times the key. Process of these cipher can be done quite quickly by hand, and even more quickly with a computer. The use of nulls can also have a detrimental effect on the security of the cipher, as an interceptor can use them to identify where the end of the line is, and so have a sensible guess at the key. This can be averted by using a more common letter, such as "X", to fill the null spaces, as it will still be clear to the recipient that these are not part of the message as they will appear at the end of the plaintext. The Rail Fence Cipher can also be utilised without the use of nulls.